



Plano de Gestão de Incidentes de Segurança da Informação Conselho Federal dos Técnicos Industriais

1. Apresentação

O presente documento está alinhado à Política de Segurança da Informação do Conselho Federal dos Técnicos Industriais.

O tratamento de ameaças e incidentes de Segurança da Informação é fundamental para evitar ataques e vazamentos que possam resultar na perda, danos ou acesso não autorizados às informações e dados, assim como mitigar os impactos causados pelo incidente.

As diretrizes aqui estabelecidas visam garantir a confidencialidade, integridade e disponibilidades das informações e dados tratados pelo CFT, respeitando as legislações vigentes.

2. Histórico de Elaboração e Aprovação

NOME	SETOR	RESPONSABILIDADE	DATA
Camila Alves de Oliveira	Gerência CSC	Elaboração	02/03/2021
Eduardo Bimbi	Gerência CSC	Revisão	04/03/2021
André Soares de Carvalho	PROJUR	Revisão	11/03/2021

3. Objetivo

O Plano de Gestão de Incidentes de Segurança da Informação do Conselho Federal dos Técnicos Industriais tem como objetivo apresentar os procedimentos e diretrizes a serem tomados nas fases de detecção, resolução, prevenção e redução da ocorrência de incidentes dos sistemas e serviços internos.

Todos os processos envolvidos na gestão de incidentes, desde a detecção até a resposta, asseguram a documentação e existência de logs adequados que permitem melhores evidências forenses e conteúdo para auditoria.

A documentação é armazenada em conformidade com as legislações vigentes e com a devida preservação de dados pessoais e sigilosos envolvidos.



4. Papéis e Responsabilidades

Os prestadores de serviço devem garantir a existência de níveis de confidencialidade e segurança que assegurem que os profissionais e serviços sob a responsabilidade do CFT estarão em conformidade com a política e as normas de segurança da informação, devendo constar cláusula de adesão a esta regra em seus contratos.

Ator	Papeis	Responsabilidades
Diretoria	Alta administração do Conselho Federal dos Técnicos Industriais.	Análise final e deliberação sobre as ações e diretrizes a serem realizadas para a solução do incidente de segurança.
Grupo Gestor LGPD	Comitê formado por integrantes do CFT e Regionais, que são responsáveis pela coordenação das ações deliberadas à luz do cumprimento da LGPD.	Analisar e deliberar sobre as ações e diretrizes a serem realizadas para a solução do incidente de segurança.
Encarregado de Dados	Membro do Grupo Gestor LGPD e nomeado como Encarregado de Dados, responsável por encaminhar comunicações formais em incidentes envolvendo dados pessoais	Elaborar relatório formal de incidente de segurança da informação. Responsável por encaminhar comunicações formais em incidentes envolvendo dados pessoais. Contato com a Autoridade Nacional de Proteção Dados Pessoais e com o titular dos dados. Revisão das normas relativas à Segurança da Informação.
Setor de Tecnologia da Informação	Equipe interna e empresas terceirizadas responsáveis pelas atividades relacionadas ao fornecimento de serviços, tratamento e resposta a incidentes de SI.	Monitorar os sistemas, a fim de identificar possíveis incidentes. Investigar o incidente de segurança da informação. Realizar análise do incidente, de forma a propor medidas para solucionar e eliminar os problemas causados. Assessorar o encarregado de dados e o Comitê na análise e decisões a respeito de incidentes de segurança da informação.



Colaboradores dos demais setores	Funcionários do CFT e regionais.	Seguir normas de segurança internas. Evitar e monitorar incidentes.
-----------------------------------------	----------------------------------	---------------------------------------------------------------------

5. Descrição das Atividades

Registrar Incidente de Segurança		
Descrição	Detectada a suspeita ou ocorrência de incidente de segurança da informação é necessário primeiramente comunicar a equipe de TI e proceder com o registro, de forma detalhada, em formulário disponibilizado. Verificar a necessidade de autorização prévia da diretoria para prosseguimento.	
Considerações	O formulário de registro do incidente deve ser preenchido o mais breve possível. De acordo com o tipo de incidente pode ser necessária a autorização prévia da Diretoria para a realização dos procedimentos necessários à investigação.	
Entrada	Comunicação ou detecção de suspeita ou ocorrência do Incidente de Segurança da Informação através de E-mail, telefone ou contato direto com o Gestor da área de TI do CFT.	
Saídas	Formulário preenchido	
Atividades	Comunicação sobre o Incidente	Encaminhamento E-mail, telefone ou contato direto com o Gestor da área de TI do CFT com as informações iniciais do incidente para Encarregado de Dados.
	Deteção do Incidente	Averiguação do incidente através de monitoramento dos sistemas.
	Esclarecimentos com o responsável pela sinalização da suspeita ou ocorrência do incidente	Contato para obter mais informações ao registro.
	Registro do Incidente	Preenchimento do Relatório de incidente e categorização do mesmo.
	Verificar necessidade de autorização prévia com a Diretoria	Após registro do incidente, verificar a necessidade de autorização da Diretoria.



	Encaminhar incidente para investigação	Encaminhar incidente para equipe de TI para início das tratativas do incidente.
--	-----------------------------------------------	---------------------------------------------------------------------------------

Encaminhar solicitação para Autorização		
Descrição	Após o registro da suspeita ou ocorrência do incidente, o relatório deve ser encaminhado para a equipe de TI e seguinte para a diretoria para análise.	
Entrada	Encaminhamento do Registro de Incidente	
Saída	Solicitação de autorização à Diretoria para início das atividades corretivas	
Atividades	Coletar as informações necessárias ao encaminhamento do pedido de autorização para prosseguimento das atividades corretivas	Solicitação de autorização à Diretoria para início das atividades corretivas.
	Prestar Esclarecimentos, quando necessário	A Diretoria poderá solicitar esclarecimentos antes da deliberação. Neste caso, o encarregado de Dados é responsável pela coleta de informações e encaminhamento à Diretoria.
	Encaminhar Registro de Incidente para tratativa	Se o registro de incidente foi aprovado pela Diretoria, deve-se encaminhar para tratativa pelo setor responsável.
	Encaminhar Registro de Incidente para finalização	Se o registro de incidente foi negado pela Diretoria, deve-se encaminhar para encerramento do incidente.

Investigar Incidente	
Descrição	A equipe técnica de TI do CFT e das empresas terceirizadas deverão investigar as possíveis causas, gravidade e impacto do incidente com base nas informações registradas inicialmente através do Relatório.



Considerações	Solicitação de informações poderão ser solicitadas para colaboradores de outras áreas. Nesta etapa do processo, é importante que seja identificado o tipo do incidente e o impacto causado para que seja dado o encaminhamento às medidas de contenção e de comunicação.	
Entradas	Autorização da Diretoria e Relatório inicial preenchido	
Saídas	Relatório com as informações investigadas	
Atividades	Verificar tipo de incidente	Verificar a causa do incidente, se foi causado por fator externo ou interno (vírus, ataques hacker, acesso não autorizado, vazamento de dados).
	Analisar grau de impacto do incidente	Análise de quais ativos foram afetados pelo impacto. Verificar os danos causados.

Ações de Contenção		
Descrição	Após investigação das causas do incidente, a equipe Técnica deverá propor as medidas para conter e solucionar o incidente.	
Considerações Importantes	As ações de solução propostas pela equipe Técnica deverão ser devidamente aprovadas pela Diretoria. Dependendo do grau de impacto, outras áreas do CFT poderão ser envolvidas, de modo em que a resolução do incidente seja o mais breve possível.	
Entradas	Propostas de medida de contenção	
Saídas	Deliberação da Diretoria	
Atividades	Propor medidas de contenção	A equipe de TI deverá propor as medidas de contenção do incidente, com base nas informações levantadas no processo de investigação. Em casos de indisponibilidade do sistema, as ações desse processo devem reestabelecer o serviço, mesmo que parcialmente a princípio.
	Encaminhar Solução para chefia	Dependendo do teor da ação proposta, a equipe de TI deverá encaminhar as ações para prévia autorização da chefia imediata e Diretoria.



	Novas medidas em casos onde o incidente não foi contido.	Caso o incidente não seja contido com as primeiras propostas de ações, novas medidas deverão ser avaliadas e aplicadas.
--	-----------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------

Notificação ANPD e Titular dos Dados		
Descrição	Após deliberação da Diretoria, deve-se analisar se o incidente envolve dados pessoais. Em caso positivo, necessário notificação formal à ANPD e ao titular dos Dados	
Entrada	Análise do Registro do Incidente através do relatório elaborado	
Saída	Notificação formal à ANPD e ao titular dos dados	
Atividades	Análise do Impacto aos Dados Pessoais	Com o incidente evidenciado, é necessário análise para averiguação se houve dano ao dado pessoal de técnicos ou colaboradores. Avaliar internamente o incidente, e apurar a natureza, categoria e quantidade de titulares de dados afetados. Além disso, na avaliação interna também devem constar as consequências concretas e prováveis do incidente.
	Notificação à ANPD e ao titular dos dados	Constatado que no incidente de Segurança da Informação houve danos em Dados Pessoais, é necessário enviar relatório de notificação a ANPD e ao titular dos dados, com as circunstâncias e impacto da violação. Notificação realizada pelo Encarregados de Dados.
	Notificação ao titular dos dados	Constatado que no incidente de Segurança da Informação houve danos em Dados Pessoais, é necessário enviar relatório de notificação ao titular dos dados, com as circunstâncias e impacto da violação. Notificação deve ser realizada pelo Encarregados de Dados.



Aplicar Medidas Aprovadas	
Descrição	Executar as ações aprovadas na fase de propostas, visando conter o incidente e analisar se o resultado gerado é suficiente e o esperado.
Considerações Importante	Após aplicar as medidas, a equipe responsável deverá informar às chefias se o incidente foi contido. Em casos negativos, novas medidas ações deverão ser realizadas.
Entradas	Documento com a aprovação das medidas
Saídas	Relatório com o resultado das medidas aplicadas
Atividades	Aplicar as medidas necessárias Realização das medidas necessárias para resolução ou contenção do incidente.
	Avaliar medidas aplicadas Verificar se o resultado das ações aplicadas foi positivo ou negativo. Em caso negativo, novas medidas deverão ser adotadas.

Análise do Incidente	
Descrição	Após contenção do incidente, o mesmo deverá ser analisado como um todo, a fim de que o processo seja finalizado e não hajam novas ocorrências similares.
Considerações Importante	A análise do incidente deve ser realizada em todas as áreas do CFT, e em caso onde o incidente foi oriundo de uma ação interna ou descumprimento da Política de Segurança Interna, os responsáveis serão passíveis de sanções que incluem advertência verbal, advertência por escrito, suspensão e a demissão por justa causa, a depender de cada caso.
Saídas	Relatório de análise do incidente



Atividades	Analisar a Causa-raiz do incidente	Auditoria de todo o cenário do incidente e identificar a porta de entrada do incidente. Verificar as vulnerabilidades exploradas, quais ameaças envolvidas, riscos e impactos.
	Propostas de melhorias	Após auditoria do cenário, propor ações de melhorias, de forma a evitar novas ocorrências.
	Elaboração do Relatório de Incidente	Elaboração do relatório de análise e encaminhamento para o Encarregado de Dados e, posteriormente para a deliberação da Diretoria.

Encerrar Incidente

Descrição	Nesta etapa do processo, deve ser analisado se as ações corretivas foram suficientes para resolução do incidente. Deve ser analisado se não há evidências ainda pendentes. Depois, o processo do incidente de segurança deverá ser finalizado.	
Considerações Importantes	Encerramento do incidente após deliberação da Diretoria Executiva	
Entrada	Deliberação da Diretoria	
Saídas	Relatório encerramento do incidente	
Atividades	Encerrar Incidente	Na inexistência de novas ocorrências ou pendências, o incidente deverá ser encerrado.
	Cumprir providências	O Encarregado de Dados deverá dar prosseguimento à notificação de encerramento do incidente aos envolvidos e à ANPD, utilizando os procedimentos definidos pela própria Autoridade Nacional de Proteção de Dados Pessoais.



Gerar Relatórios de Evidências		
Descrição	Independentemente do tipo de incidente ou gravidade do mesmo, é necessário que seja elaborado relatório com as evidências do evento, desde a identificação à resolução.	
Considerações Importantes	Sempre que o relatório envolve dados pessoais, o documento deverá ser protegido e armazenado em local restrito.	
Entradas	Informações obtidas desde o inicial do processo	
Saídas	Relatório de Evidência de Incidente	
Atividades	Identificação dos dados necessários para elaboração do Relatório de Evidência do Incidente	Identificação das informações que melhor podem elucidar a questão noticiada com todos os envolvidos no processo.
	Coleta e compilação dos Dados	Realizar a coleta e compilação dos dados necessários à elaboração do Relatório. Essas informações devem ser protegidas e o acesso deve ser restrito apenas aos envolvidos direto na elaboração.
	Elaboração do Relatório de Evidência do Incidente	Com base nos dados coletados, inicia-se a elaboração do relatório de evidência.
	Aprovação do Relatório de Evidência do Incidente	Após elaborado, o relatório deve ser revisado pelo encarregado de Dados e encaminhado à Diretoria para aprovação do documento.

Oportunidade de Melhorias		
Descrição	Análise de todo o histórico de incidente, de forma a evidenciar possibilidades de melhorias nos serviços e no processo de tratativa de incidente de Segurança da Informação.	
Considerações Importante	A ação de análise de melhoria no processo de gestão de incidentes deverá ocorrer periodicamente e não apenas quando evidenciado um incidente de Segurança da Informação.	
Saída	Relatório de melhorias	
Atividades	Análise de histórico	Análise com a equipe técnica ou relatórios anteriores para verificação de possíveis vulnerabilidades e ameaças nos sistemas e processos.



	Oportunidade de melhoria	Com base na análise realizada, novas ações para melhorar o processo deverá ser apontada.
	Implantar Melhorias	Planejar e aplicar as melhorias identificadas.

6. Riscos e Ameaças

Considera-se RISCO, qualquer evento que possa causar impacto no CFT, gerando assim um Incidente.

Um Incidente de Segurança da Informação é qualquer evento que não faz parte da operação padrão para funcionamento dos serviços do CFT e que causa ou pode causar a interrupção desses serviços. Acontece quando um dos pilares da Segurança da Informação é quebrado.

Nenhum sistema é 100% seguro, motivo pelo qual os serviços oferecidos pelo Conselho Federal dos Técnicos Industriais são passíveis de ataques externos e/ou internos.

Dentre os riscos e ameaças ao qual os serviços do CFT estão suscetíveis, priorizamos como ameaças Externas a possibilidade de Ataques Hackers, Softwares vulneráveis, Acidentes físicos, dentre outros.

Dentre os tipos de riscos e ameaças internas, destacam-se os riscos à proteção de dados e informações armazenadas pelo CFT, em especial aos dados pessoais.

Esse tipo de risco pode ser descrito como potencial evento que gera impacto sobre o titular de dados pessoais e sobre o próprio CFT. Estão basicamente ligados às vulnerabilidades internas. Listamos os seguintes como principais:

- I. **Acesso não autorizado:** Acesso aos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
- II. **Modificação não autorizada:** Modificação de dados pessoais sem a anuência do titular. Viola o princípio da segurança.
- III. **Perda:** Destruição ou extravio de dados pessoais. Viola os princípios da segurança e da prevenção.
- IV. **Apropriação:** Apropriação ou uso indevido de dados pessoais. Possibilidades de fraude e vazamento intencional de dados. Viola os princípios da segurança e da prevenção.
- V. **Remoção não autorizada:** Retirada de dados pessoais sem autorização do titular.
- VI. **Coleta excessiva:** Extração de mais dados do que o necessário para a realização do tratamento, ou do que é previsto em Lei ou autorizado pelo titular. Viola o princípio da necessidade.



- VII. **Informação insuficiente sobre a finalidade do tratamento:** A finalidade declarada para o uso das informações pessoais é insatisfatória, não é específica ou pode suscitar interpretações diversas.
- VIII. **Tratamento sem consentimento do titular dos dados pessoais:** Tratamento dos dados pessoais sem o prévio consentimento expresso, inequívoco e informado do titular, salvo exceções legais.
- IX. **Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais:** Compartilhamento dos dados pessoais com outras entidades privadas sem a devida permissão do titular.
- X. **Retenção prolongada de dados pessoais sem necessidade:** Manter os dados pessoais do titular para além do necessário ou do que estava consentido/autorizado. Viola o princípio da necessidade.
- XI. **Vinculação ou associação indevida, direta ou indireta, dos dados pessoais ao titular:** Erro ao vincular dados do verdadeiro titular a outro. Viola o princípio da qualidade dos dados.
- XII. **Falha ou erro de processamento:** Processamento dos dados de forma imperfeita ou equivocada. Viola o princípio da qualidade dos dados.
- XIII. **Reidentificação de dados pseudonimizados:** Anonimização insatisfatória de dados pessoais, em especial as sensíveis, possibilitando inferir quem é a pessoa em questão. Viola o direito à anonimização.

7. Considerações Finais

Conforme metodologias ITIL de gestão, o Plano de Gestão de Incidentes de Segurança da Informação do CFT tem como objetivo restaurar as operações de serviço o mais breve possível, de modo que seus impactos no CFT e aos titulares de dados sejam minimizados.

O Plano de Gestão de Incidentes de Segurança da Informação tem abrangência em todos as áreas do CFT, de modo que todos os colaboradores internos, prestadores de serviços e empresas terceirizadas tenham ciência do impacto que um incidente pode causar ao CFT, e ter conhecimento sobre a importância de sua atuação nos processos de identificação, contenção e resolução do incidente.

As ações de resolução de um incidente de Segurança da Informação são focadas na eficiência do processo, de modo que relatórios e resultados criados são armazenados para referência futura.



8. Revisão e Atualização do Plano de Gestão de Incidentes de Segurança da Informação

O presente documento deve ser revisto e atualizado anualmente, alinhado sempre às legislações e regulamentos vigentes.

O atual Plano foi aprovado em XXXXX

